Security Overview

- System protection requirements areas
- Types of information protection
- Information Architecture dimensions
- Public Key Infrastructure (PKI)

Information Protection Requirements

- Confidentiality
  - Protect from unauthorized disclosure
- Integrity
  - Protect from unauthorized modification
- Availability
  - Reliable/timely access to required resources
- Authenticity
  - Ability to determine authorized source
- Non-repudiation
  - Non-forgeable proof of data originator’s identity and data receipt

Types of Information Protection

- Encryption
- Access control
- User identification and authentication
- Malicious content detection (viruses)
- Audits, including real-time intrusion-detection
- Physical Security

Information Architecture Dimensions

- Information System
  - Unauthorized intrusion
  - Denial of service
- Information Domain
  - Users must have freedom of movement within their authorized spheres
- Information Content
  - In-transit
  - At rest

PKI
Public Key Infrastructure

- Generation of digital certificates
  - Electronic proof of identity
- Issuance of Certificate Revocation Lists (CRLs)
- Directories that serve certificates and CRLs

PKI Terms

- Certificate Authority (CA): Trusted agent that signs and issues digital certificate
  - Sets rules for use,
  - Publishes CRLs,
  - Posts to directory server
- Registration Authority (RA): Verifies person’s identity, passes on to CA

Defense Messaging System

- PKI by itself is considered medium grade security assurance
- DMS involves PKI with modifications and additions
  - DMS is considered “high grade” assurance
- Includes detailed policies and custom software
- http://www.disa.mil/D2/dms/

Further reading

- DON CIO Information Technology Standards Guidance (1999)– Chapter 3
  - http://www.doncio.navy.mil/training/ools/itsg/chapter3.html
- DoD Computer Emergency Response Team (CERT)
  - http://199.211.123.12/